# System Security

## ZENworks® Mobile Management 2.8.x

**September 2013**

Novell®

## Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.



Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

*Online Documentation:* To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

## Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

## Third-Party Materials

All third-party trademarks are the property of their respective owners.

# Table of Contents


## Architecture 4

## ZENworks Mobile Management System Security 6

Server-to-Server Data Transmission Security ....6
Database Security: Data-at-Rest Encryption ....6
Server Log Security ....7
Device-to-Web/HTTP Server Data Transmission Security ....9
Implementation Guidelines: Device-to-Server Data Transmission Security ....9
Device Security ....10
Implementation Guidelines: Preventing Device Breaches ....13

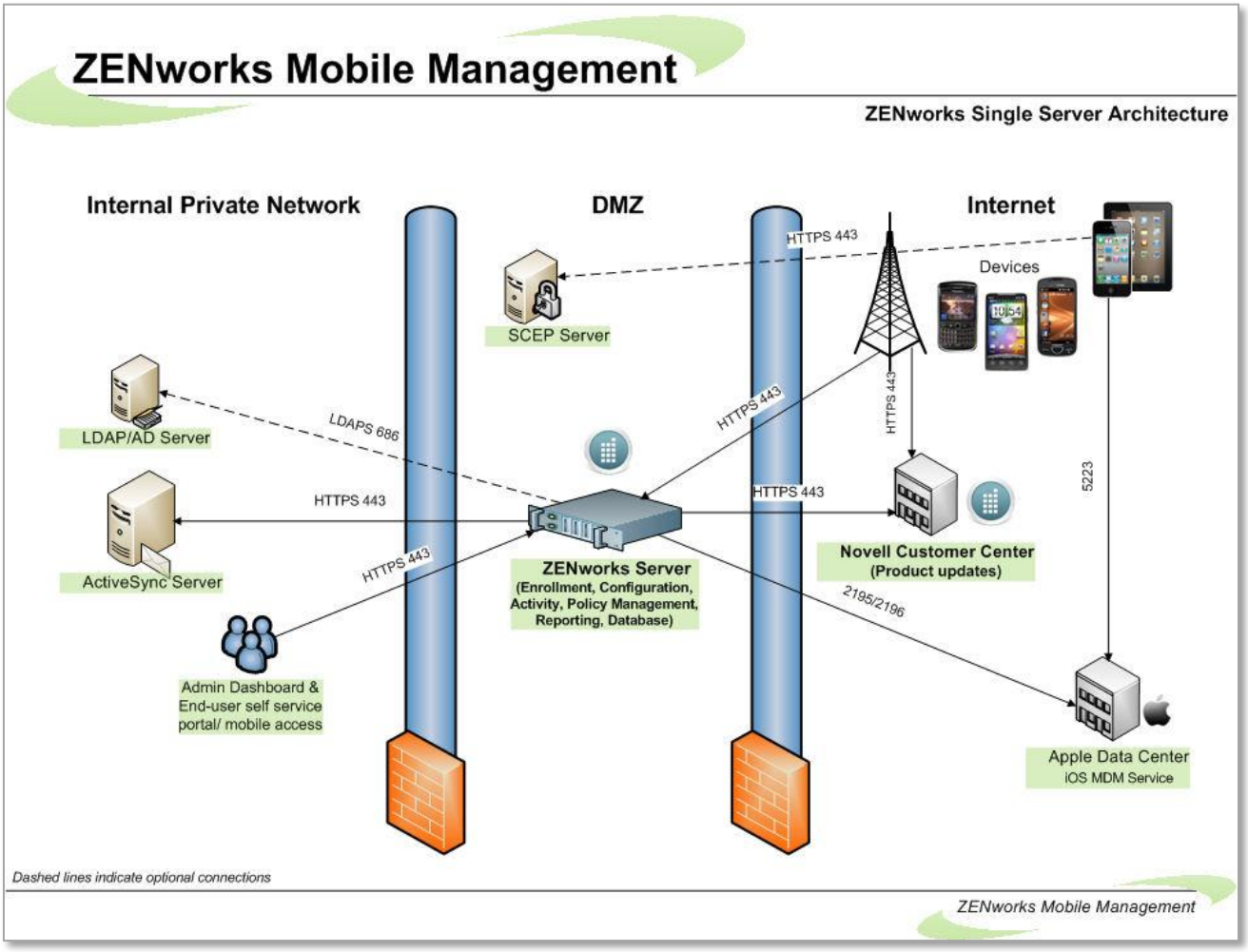
# Architecture

*ZENworks Mobile Management* consists of an ***SQL Database Component*** and a ***Web/HTTP Server Component***. The components might be installed on a single server or multiple servers. The architecture you choose depends on system size and complexity.

In addition to the setups illustrated below, a reverse proxy setup is also supported if the proxy is sufficiently scalable. For the long term, redundant proxies might be advisable to help ensure high availability. Achieving redundancy through SQL and Web clusters is a good way to ensure high availability.

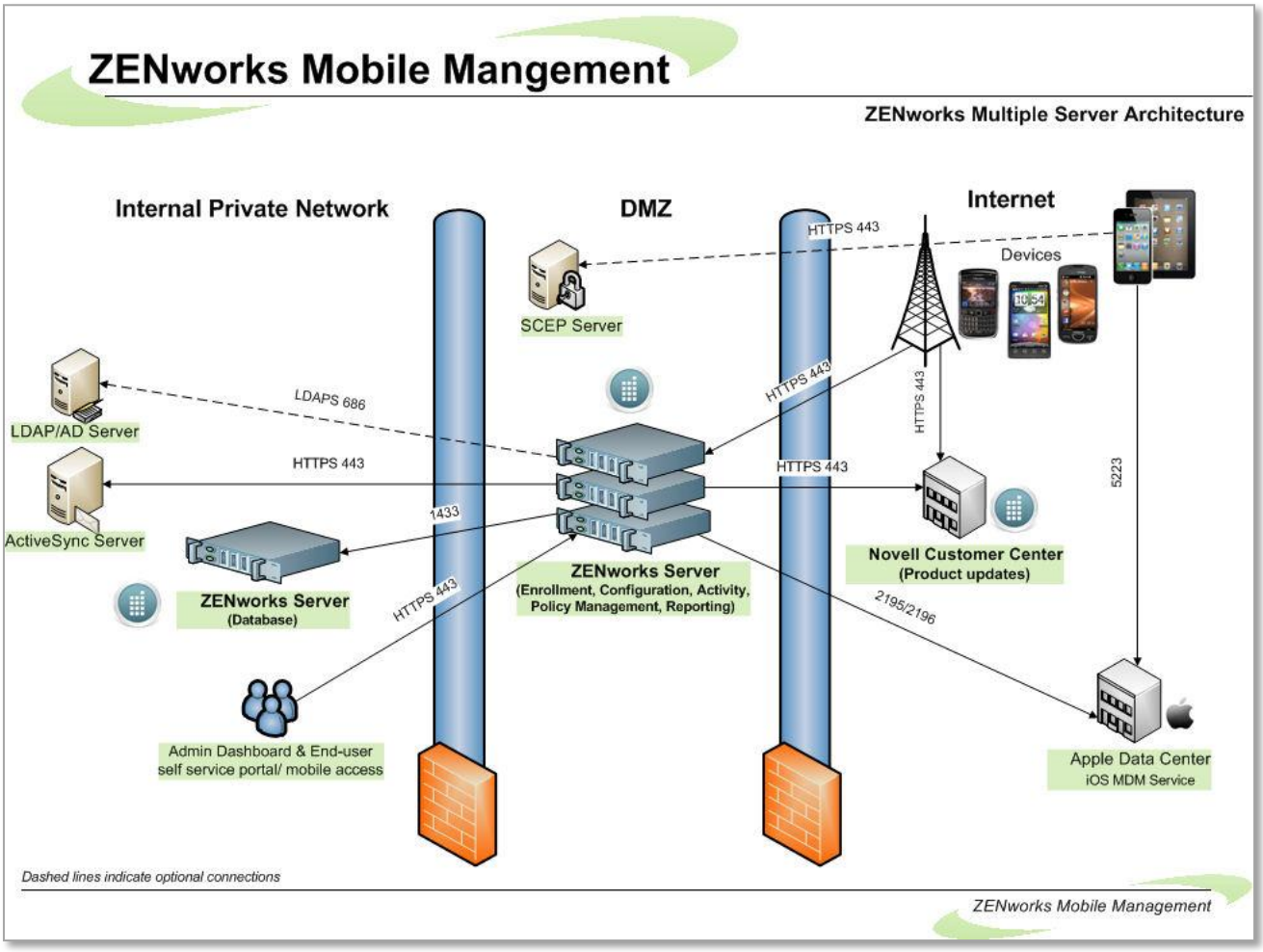
### Single Server Configuration Diagram

*Typical configuration suitable for general-purpose deployment where a single server meets all the requirements needed for installation.*



### Multiple Server Configuration Diagram

*Deployment options for larger, more complex deployments where a single server does not meet all the requirements needed for installation.*




See related topics:
[System Performance: Sizing/Tuning]

[High Availability Configuration]

To simplify a description of the *ZENworks Mobile Management* security system, we have grouped the security features into several categories, which we refer to as the “layers” of security.

- Server-to-Server Data Transmission Security
- Database Security: Data-at-Rest Encryption
- Server Log File Security
- Device-to-Server Data Transmission Security
- Device Security

# ZENworks Mobile Management System Security

**Terms:**

**SSL Encryption**: Secure Socket Layer Security. Using SSL to secure data exchanges provides an encrypted tunnel between the ZENworks Mobile Management servers and other servers or devices.

**TLS Encryption**: Transport Layer Security Encryption. TLS is a FIPS 140-2 compliant encryption protocol that provides an encrypted tunnel through which sensitive data can travel. You can enable TLS through IIS. However, this might limit the types of devices that can connect to the ZENworks Mobile Management server because not all devices support TLS.

## Server-to-Server Data Transmission Security

**ZENworks Mobile Management requires the use of SSL or TLS** with the servers where the *ZENworks Mobile Management Web/HTTP* component is installed, to meet best practices for security. ZENworks Mobile Management supports the use of SSL or TLS certificates from trusted Certification Authorities to ensure secure server-to-server data transmission.

- Server-to-server connections within the Internal Private Network might include connections between:
    - ActiveSync server and ZENworks Mobile Management server
    - LDAP/AD server and ZENworks Mobile Management server
    - SCEP server and ZENworks Mobile Management server
- Connections from ZENworks Mobile Management server to servers outside the Internal Private Network includes:
    - ZENworks Mobile Management server to ZENworks Mobile Management Customer Center (product updates, etc.)
    - ZENworks Mobile Management server to Apple Data Center

## Database Security: Data-at-Rest Encryption

Sensitive data-at-rest is secured in the *ZENworks Mobile Management* database by using the AES encryption algorithm. *ZENworks Mobile Management* servers use a 256-bit encryption key size to encrypt user information in the database. *ZENworks Mobile Management*'s procedures for key storage and key derivation are FIPS compliant.

Encrypted database information includes:

- Passwords
- User Encryption Key
- Authentication Password (stored only if authenticating via *ZENworks Mobile Management*, not ActiveSync)
- Text Message Log (can be disabled so it is not sent to the server)
- Location Data (can be disabled so it is not sent to the server)

- Phone Log (can be disabled so it is not sent to the server)
- Device Logging (can be disabled so it is not sent to the server)
- File Archive (can be disabled so it is not sent to the server)

The *ZENworks Mobile Management* database component itself is secured by using built-in SQL Server security features. By default, *ZENworks Mobile Management* creates a single SQL Server login with access to the *ZENworks Mobile Management* database. Permissions can be set within SQL Server, as desired, to access the database by other SQL Server logins or by using Windows Authentication.

# Server Log Security

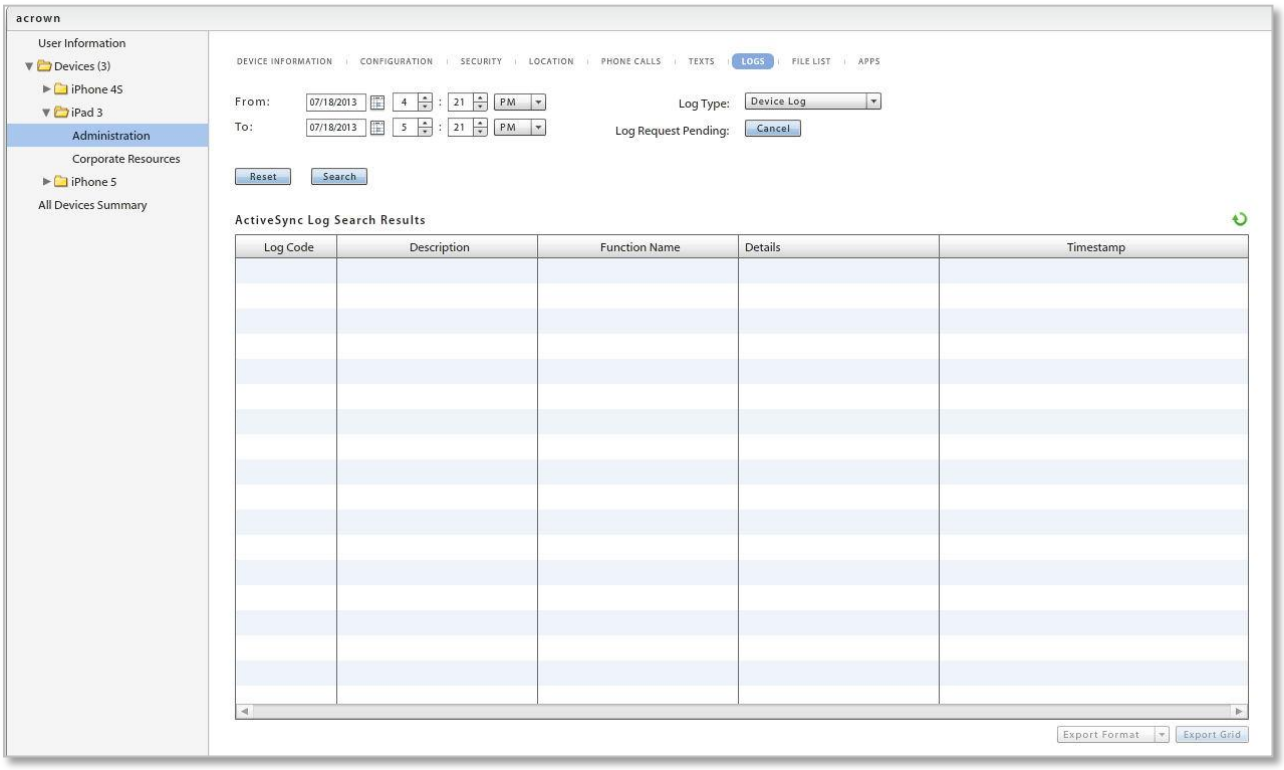
*ZENworks Mobile Management Server* error logging is intended to be used as a diagnostic tool by the Novell Technical Support staff.

Servers where the log files reside should be secured. In addition, administrators should limit access to the directory where the logs are contained.

Server logs are displayed in the *ZENworks Mobile Management* Dashboard and access to these views can be restricted via administrative login credentials. The data displayed in the Server Logging page of the dashboard is system-level data and has no user associations. Displayed logging information that is associated with users is limited to *ZENworks Mobile Management* and ActiveSync synchronization data.

There is also a log file stored on the server that is not dependent on access to the database tables. This is secured by standard Windows authentication and file system security configurations.

In the user profile, there is also a way to request user level logs from the device. These logs assist administrators with diagnosing problems and in understanding the communications between devices and the server.




*User Profile: Device Log*

For **BlackBerry** (with *NotifySync for BlackBerry*), **iOS, Symbian, and Windows Mobile platforms**, a log file only has *ZENworks Mobile Management*-specific log-entries.

Examples of log entries for BlackBerry (with *NotifySync for BlackBerry*), iOS, Symbian, and Windows Mobile:

- Beginning Sync
- Ending Location Sync
- Beginning Device Log Sync
- Ending Device Log Sync
- Registration status code: 200
- Reg - Account Removed
- DeviceStats returned: 200
- GetAppListConnection returned: 200
- Account loading

For **Android**, a log file has log-entries encompassing ZENworks Mobile Management-specific logs, device log, and the log entries from Touchdown (if TouchDown is installed and registered).

Examples of log entries for Android:

- ConnectivityChange for mobile: CONNECTING/CONNECTING
- ConnectivityChange for mobile: CONNECTED/CONNECTED
- DISABLE_CLOCK: yes
- DISABLE_NAVIGATION: yes
- Attempting to switch to WIFI
- Attempting to switch to BLUETOOTH_TETHER
- Scheduling restart of crashed service
- SyncHandler: Attempting to send device location command

# Device-to-Web/HTTP Server Data Transmission Security

Device-to-Web/HTTP server data transmission must be secured by employing SSL or TLS. With SSL or TLS enabled, *ZENworks Mobile Management* transmits “data-in-motion” (information originating on a device or server) in an encrypted tunnel so it is secure in transit.

Data-in-motion includes both *ZENworks Mobile Management* traffic and ActiveSync server traffic that is proxied by the *ZENworks Mobile Management* server.

In extreme cases or where certain security standards are imposed, you might want or need to further secure the Web/HTTP server by locking down the virtual directories. Access to the *ZENworks Mobile Management* dashboard and the User Self-Administration Portal from external sources can be blocked. Pages accessed by mobile devices for synchronization, however, must be kept open. See instructions for locking down the virtual directories below.

Connections to the *ZENworks Mobile Management* server made by users might also include:

- Administrative access from sources either inside or outside the Internal Private Network via the Web-based ZENworks Mobile Management Dashboard to a ZENworks *Mobile Management* server.
- Desktop or mobile access from sources either inside or outside the Internal Private Network via the Web-based ZENworks Mobile Management User Self Administration Portal to a ZENworks *Mobile Management* server.

These connections can also be secured using SSL or TLS.

All data-in-motion can be secured using the SSL or TLS protocols. The device side has SSL and the server side has the options of SSL or TLS (the server automatically negotiates the best option, and hence uses TLS most of the time).

## Implementation Guidelines: Device-to-Server Data Transmission Security

**Enable SSL for Device-to-Web/Http server communication.**

- Install an SSL certificate on the server where the *ZENworks Mobile Management* Web/HTTP component resides and enable SSL (or TLS) in IIS.
- Use the *Require SSL* option through IIS and instruct users to enroll with SSL enabled or enable it in the device settings.

**Secure the Web/HTTP server by locking down virtual directories.**
In extreme cases or where certain security standards are imposed, you might want or need to further secure the Web/HTTP server by locking down the virtual directories.

1. Open Windows Server Internet Information Services (IIS) Manager
2. Expand the directory and select **Sites** > **Default Web Site**.
3. At the root level, double-click **IP Address & Domain Restrictions**. (If *IP Address & Domain Restrictions* is not present, you must install the *IP and Domain Restrictions Role*. Right-click *Computer* and select *Roles*. Under the *Web Server (IIS)* section, click *Add Role Service*. Install the *IP and Domain Restrictions* role under *Security* in the popup window.)
4. From the *Actions* panel on the right, click **Edit Feature Settings** and set the value to **Deny**.
5. From the *Actions* panel, click **Add Allow Entry** and add the following rules to allow only *local* access to the dashboard and User Self-Administration Portal:
    a. IP: (the internal IP address of the *ZENworks Mobile Management* Server)
    b. IP: 127.0.0.1

    Add any other IP address, from which you will allow access, in the same manner.
6. The IP addresses that you added to the root level automatically populate for all the subdirectories, however, the *Feature Settings* value must be manually set to *Deny* for all but the *Sync* subdirectory. Select each *Default Web Site* subdirectory, **except *Sync***, and double-click *IP Address & Domain Restrictions*. Set the *Edit Feature Settings* to **Deny**.

# Device Security

*ZENworks Mobile Management* device security implements proactive features that can help deter security breaches. It also includes reactive security options that can be implemented when a device is lost or stolen and therefore more vulnerable to a breach.

This section highlights *ZENworks Mobile Management's* core device security features.

## Proactive Device Security Options

### Device Data-at-Rest Encryption

Data-at-rest encryption on the device storage disk is supported by several device types and can be enforced through the *ZENworks Mobile Management* Policy Suite.

- Android with TouchDown – Encrypts TouchDown data (email, calendar, contacts, tasks) only
    - Versions 7.x and higher – AES 256-bit
- Android (Native) devices - OS version 3.0; manufacturer/model dependent for OS versions less than 3.0
    - AES 128-bit
- BlackBerry – (with *NotifySync for BlackBerry)* encrypts the *NotifySync* email
    - Secure (AES 128-bit)
    - More Secure (AES 192-bit)
    - Most Secure (AES 256-bit)
- iOS Devices – AES 256 bit
    - iOS4 (3GS and 4) and iOS5 devices have hardware encryption that is always enabled. The ActiveSync policy is not used to enable/disable.
- Symbian S60 3rd edition devices – 256 bit
- Windows Mobile 6.1 and 6.5 – AES 128-bit
- Windows Phone 7 – This device does not currently support Data-at-Rest encryption.

### Device Rules: Lock Rules

#### Inactivity Timeout

- *BlackBerry(*with *NotifySync for BlackBerry), iPhone/ iPod touch/ iPad, Windows Mobile, Symbian, Android Native, Android with TouchDown, and Windows Phone 7 platforms*
  The maximum inactivity timeout can be enforced by the server and an interval that does not exceed this maximum can be set on the device.

#### Challenge Timeout

- *BlackBerry (*with *NotifySync for BlackBerry)*

  The *ZENworks Mobile Management* Challenge Timeout lock is initiated regardless of inactivity and is intended to challenge the use of the device if it is lost or stolen. It must be greater than the *Inactivity Timeout*.
- *iPhone/ iPod touch/ iPad, Windows Mobile, Symbian, Android Native Android with TouchDown, and Windows Phone 7 platforms* – Not supported

#### Duress Notification

- *BlackBerry* (with *NotifySync for BlackBerry)*
  If enabled, this option allows the user to activate the duress notification if he/she is forced to unlock the device under duress by entering the password in an altered format (shift all characters to the left). For example: If lock password is “guarddog”, the duress password is “uarddogg”.

  A high priority email notification is sent to the specified email address with the Subject: “*ZENworks Mobile Management* Duress Notification.” The notification is completely hidden from view. It does not appear in the Outbox, Sent Items, or Deleted Items folders.

- *iPhone/ iPod touch/ iPad, Windows Mobile, Symbian, Android Native Android with TouchDown and Windows Phone 7 platforms* – Not supported

### Device Rules: Password Rules

#### Device Password Expiration

- *BlackBerry* (with *NotifySync for BlackBerry), iOS Device, Windows Mobile, Android Native (some models), Android with TouchDown, and Windows Phone 7 Platforms*
  If enabled, user is prompted to create a new password after a specified number of days. When the password expires, the device locks. The user must unlock it with the current password and then create a new password at the prompt.

- *Symbian S60 3 Devices* – Not supported

#### Device Password History

- *BlackBerry* (with *NotifySync for BlackBerry), iOS Device, Windows Mobile, Android Native (some models), Android with TouchDown, and Windows Phone 7 Platforms*
  If enabled, this feature prevents users from reusing passwords too soon. On BlackBerry (with *NotifySync for BlackBerry)*, iOS, Windows Mobile, and Windows Phone 7 devices, the server can enforce the number of passwords a device should store (1 to 50). For example, if the number of stored passwords is 10, you cannot use the past ten passwords. When you create the eleventh password, the oldest stored password becomes available for use again.

- *Symbian S60 3 Devices* – Not supported

## Reactive Device Security Options

*ZENworks Mobile Management* supports remote WIPE and LOCK executions and local (device) WIPE executions (where applicable). Remote WIPE and LOCK are controlled via the *ZENworks Mobile Management d*ashboard and work when wireless is on.

#### Full Wipe

Administrators or end users can issue a Full Wipe command. Functionality varies by device.

- Android with native ActiveSync account (requires OS v2.2 or greater) – The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. The SD card is not erased.

- Android with TouchDown (requires OS v2.2 or greater) – The device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. This does not erase the SD card. When the Clean SD card on Remote Wipe option in the TouchDown Advanced Settings is enabled, the SD card is completely erased.

- Android w/TouchDown using OS v2.0 or 2.1 - You can use Selective Wipe because Full Wipe is not available.

- BlackBerry (with *NotifySync for BlackBerry)* - Removes the *ZENworks Mobile Management* account and locks the device if Require Password is enabled. It also erases the entire SD card, including saved attachments.
- iOS - Deletes all data and applications from the device. The device returns to the state it was in when purchased (factory settings).
- Symbian - Deletes all data and applications from the device. The device returns to the state it was in when purchased (factory settings). Some models (N95 and 6120c) wipe only Mail for Exchange data. This also erases the SD card.
- WM - Deletes all data and applications from the device. The device returns to the state it was in when purchased (factory settings). This erases the SD card only on Professional devices.
- WebOS and WP7 - Deletes all data and applications from the device. The device returns to the state it was in when purchased (factory settings).

### Selective Wipe

Administrators or end users can issue a selective wipe command. Functionality varies by device.

- Android w/ native ActiveSync account (requires OS v2.2 or greater) - Removes the *ZENworks Mobile Management* account information.
- Android w/ TouchDown (using any supported OS) - Removes all mail and PIM (calendar, contact, tasks) data associated with the TouchDown application and returns TouchDown to a pre-registration state. It erases TouchDown data from the SD card and removes the *ZENworks Mobile Management* account information. When the Clean SD card on Remote Wipe option in the TouchDown Advanced Settings is enabled, the SD card is completely erased.
- BlackBerry (with *NotifySync for BlackBerry)* - Removes all mail and PIM data associated with *ZENworks Mobile Management* and locks the device if Require Password is enabled.
- iOS - Removes all mail and PIM (calendar and contacts) data controlled by *ZENworks Mobile Management*. Command is applied immediately; however, device is capable of postponing the action.
- Symbian - Removes the *ZENworks Mobile Management* account information.

### Lock Device

- Administrators or end users can remotely lock the device, requiring an unlock password to be entered before the device can be used. Android and Android with TouchDown (OS 2.2 or greater), BlackBerry (with *NotifySync for BlackBerry*), iOS, and Windows Mobile support this policy.
- Symbian S60 3 and Windows Phone 7 devices – Not supported.

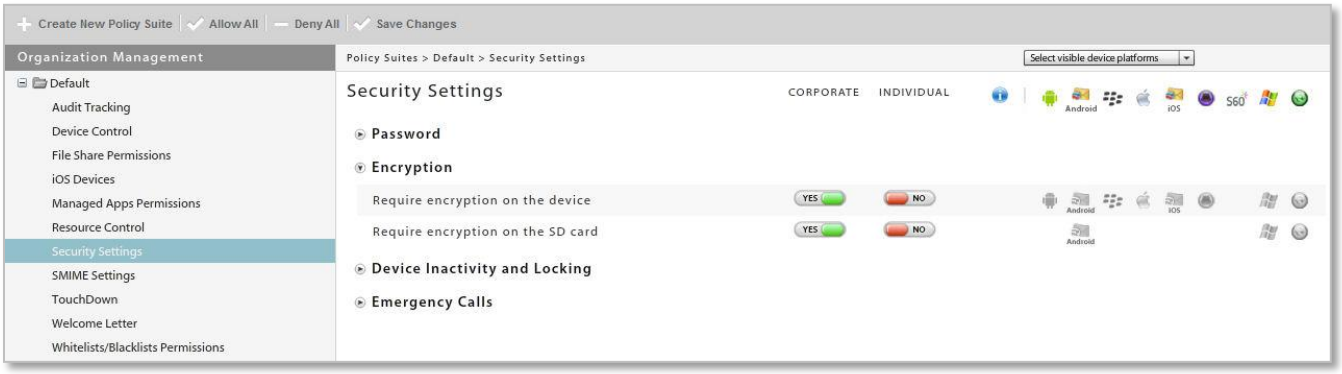
### Wipe Storage Card

- Administrators or end users can remotely wipe all data from the device's storage card. This is supported for Android, BlackBerry (with *NotifySync for BlackBerry*) and Windows Mobile platforms.

## Implementation Guidelines: Preventing Device Breaches

The *ZENworks Mobile Management* dashboard is considered the main point of control and security enforcement. From here, administrators can ensure that security is being optimally maintained through continuous monitoring of the connected user devices. All administrative actions indicated in the *Device Security* section of this document can be executed through this dashboard.

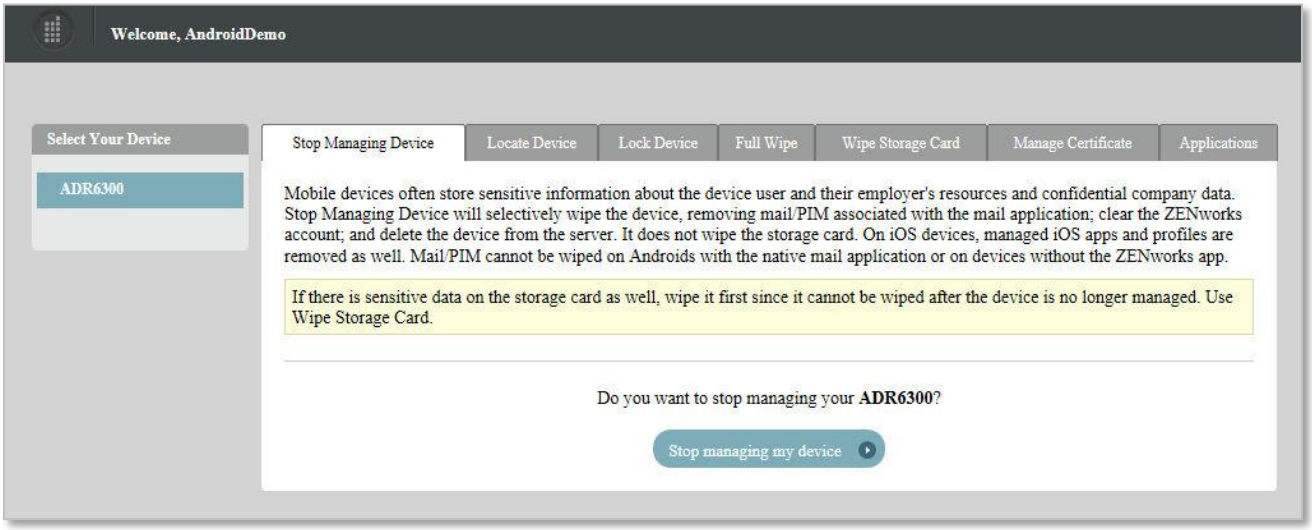
*ZENworks Mobile Management* provides a number of preventative policy settings designed to avert security breaches with regard to mobile devices. Lock, password, and encryption rules are enforced from the **Organization: Policy Suites** view of the *ZENworks Mobile Management* dashboard.




*Policy Suite: Security Settings*

Wipe and Lock commands are issued from the **Users** tab on the *ZENworks Mobile Management* Dashboard. Users might also issue the commands via the User Self Administration Portal.


*User Detail Panel*




*Desktop User Self Administration Portal*